European Journal of Molecular & Clinical Medicine

ISSN 2515-8260 Volume 09, Issue 03, 2022

ROAD ACCIDENT ANALYSIS USING MACHINE LEARNING

T.Sunitha

Associate Professor

G Durga Bhavani , V Gayathri , Sk Mastanvali , S Blessy John

B.Tech., Scholars,

Department of Computer Science & Engineering, QIS College of Engineering & Technology

ABSTRACT

In recent years, the road accident has become a global problem and marked as the ninth prominent cause of death in the world. Due to the enormous number of road accidents every year, it has become a major problem in Bangladesh. It is entirely inadmissible and saddening to allow its citizen to kill by road accidents. Consequently, to handle this overwhelmed situation, a precise analysis is required. This research paper has been done to analyse traffic accidents more deeply to determine the intensity of accidents by using machine learning approaches in Bangladesh. We also figure out those significant factors that have a clear effect on road accidents and provide some beneficent suggestions regarding this issue. Analysis has been done, by using Decision Tree, K-Nearest Neighbours (KNN), Naïve Bayes, SVM (Support Vector Machine) and AdaBoost these four supervised learning techniques, to classify the severity of accidents into Fatal, Grievous, Simple Injury and Motor Collision these four categories. Finally, the best performance is achieved by SVM.

INTRODUCTION

The problem of deaths and injuries as a result of accidents is to be a global phenomenon. [1] Traffic safety has been a serious concern since the start of the automobile age, almost one hundred years ago. [2] It has been estimated that over 300,000 persons die and 10 to 15 million persons are injured every year in road accidents throughout the world. [3] Statistics have also shown that mortality in road accidents is very high among young adults that constitute the major part of the work force. [4] In order to overcome this problem, there is need of various road safety strategies, methods and counter measures. The survey was conducted on different causes of death due to injury.

World Health Organization (WHO) report tells a horrible story that, most of the deaths between the ages 15 to 29 years are occur due to road traffic accidents and per year, more than 1.25 million people lost their lives due to road crashes. A survey from WHO reported some common reasons like shortage of training institutes, poor condition of roads as well as poor traffic management are the root causes. So to overcome this issue a systematic approach and firmly based solution is required with efficient and effective measures. So our system encounters such parameters and gives a systematic and visualizes view to overcome and interpret there spective problem.

Engineers and researchers in the automobile industry have tried to design and build safer automobiles, but traffic accidents are unavoidable. [5] Patterns involved in dangerous crashes could be detected by developing a prediction model that automatically classifies the type of injury severity of various traffic accidents. These behavioural and roadway patterns are useful in the development of traffic safety control policy.

It is important that measures be based on scientific and objective surveys of the causes of accidents and severity of injuries. The system presents some models to predict the severity of injury that occurred during traffic

accidents using machine-learning approaches. We considered networks trained using learning approaches. Experiment results reveal that among the machine learning paradigms considered various paradigms approaches.

LITERATURE SURVEY

Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT

Abstract

Cloud computing has promoted the success of Internet of Things (IoT) with offering abundant storage and computation resources where the data from IoT sensors can be remotely outsourced to the cloud servers, whereas storing, exchanging and processing data collected through IoT sensors via centralised or decentralised cloud servers make cloud-based IoT systems prone to internal or external attacks. To protect IoT data against potential malicious users and adversaries, some cryptographic schemes have been applied to ensure confidentiality and integrity of IoT data. It is however a challenging task to perform any arithmetical computations once data items are encrypted. Fully-homomorphic encryption which is based on lattices can, in principle, provide a solution, but it is unfortunately inefficient in computation and hence cannot be applied to IoT. Fully-homomorphic encryption is feasible when we allow an involvement of semi-trusted server. However, it is challenging to provide such a system in the situation of distributed environments for shared IoT data. We solve this problem and provide a fully-homomorphic encryption scheme for cloud-based IoT applications. We introduce a new method with the aid of semi-trusted server who can help in the computation of the homomorphic multiplications without gaining any useful information of the encrypted data.

Security and Privacy in IoT-Cloud-Based e-Health Systems A Comprehensive Review

Abstract

When the Internet and other interconnected networks are used in a health system, it is referred to as “e-Health.” In this paper, we examined research studies from 2017–2020 to explore the utilization of intelligent techniques in health and its evolution over time, particularly the integration of Internet of Things (IoT) devices and cloud computing. E-Health is defined as “the ability to seek, find, understand and appraise health information derived from electronic sources and acquired knowledge to properly solve or treat health problems. As a repository for health information as well as e-Health analysis, the Internet has the potential to protect consumers from harm and empower them to participate fully in informed health-related decision-making. Most importantly, high levels of e-Health integration mitigate the risk of encountering unreliable information on the Internet. Various research perspectives related to security and privacy within IoT-cloud-based e-Health systems are examined, with an emphasis on the opportunities, benefits and challenges of the implementation such systems. The combination of IoT-based e-Health systems integrated with intelligent systems such as cloud computing that provide smart objectives and applications is a promising future trend.

IoT Privacy and Security: Challenges and Solutions

Abstract: Privacy and security are among the significant challenges of the Internet of Things (IoT). Improper device updates, lack of efficient and robust security protocols, user unawareness, and famous active device monitoring are among the challenges that IoT is facing. In this work, we are exploring the background of IoT systems and security measures, and identifying (a) different security and privacy issues, (b) approaches used to secure the components of IoT-based environments and systems, (c) existing security solutions, and (d) the best privacy models necessary and suitable for different layers of IoT driven applications. In this work, we proposed a new IoT layered model: generic and stretched with the privacy and security components and layers identification. The proposed cloud/edge supported IoT system is implemented and evaluated. The lower layer represented by the IoT nodes generated from the Amazon Web Service (AWS) as Virtual Machines. The middle layer (edge) implemented as a Raspberry Pi 4 hardware kit with support of the Greengrass Edge Environment in AWS. We used the cloud-enabled IoT environment in AWS to implement the top layer (the cloud). The security protocols and critical management sessions were between each of these layers to ensure the privacy of the users’ information. We implemented security certificates to allow data transfer between the layers of the proposed cloud/edge enabled IoT model. Not only is the

proposed system model eliminating possible security vulnerabilities, but it also can be used along with the best security techniques to countermeasure the cybersecurity threats facing each one of the layers; cloud, edge, and IoT.

Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges

Abstract

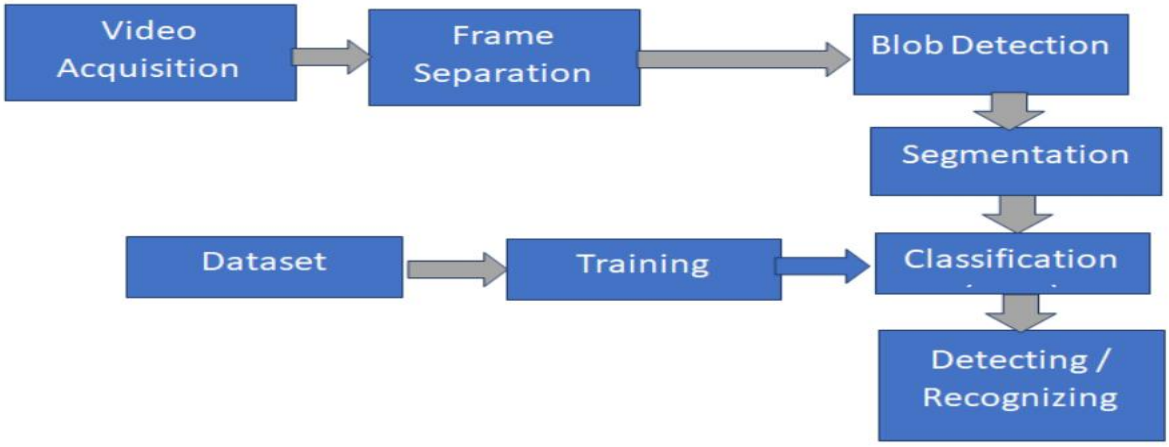
The Cloud of Things (IoT) that refers to the integration of the Cloud Computing (CC) and the Internet of Things (IoT), has dramatically changed the way treatments are done in the ubiquitous computing world. This integration has become imperative because the important amount of data generated by IoT devices needs the CC as a storage and processing infrastructure. Unfortunately, security issues in CoT remain more critical since users and IoT devices continue to share computing as well as networking resources remotely. Moreover, preserving data privacy in such an environment is also a critical concern. Therefore, the CoT is continuously growing up security and privacy issues. This paper focused on security and privacy considerations by analyzing some potential challenges and risks that need to be resolved. To achieve that, the CoT architecture and existing applications have been investigated. Furthermore, a number of security as well as privacy concerns and issues as well as open challenges, are discussed in this work.

SYSTEM ANALYSIS

Existing System:

Traffic sign detection and recognition which is necessary to be developed to support several expert systems such as driver assistance and autonomous driving system. This study focused on the detection and recognition process tested on Indonesian traffic signs. There were some major issues on detecting process such as damaged signs, faded color, and natural condition. Therefore, this paper is proposed to address some of these issues and will be done in two main processes. The first one is traffic sign detection which divided into two steps. Start with segmenting image based on RGBN (Normalized RGB), then detects traffic signs by processing blobs that have been extracted by the previous process. The second process is traffic sign recognition process. In this process there are two steps to take. The first one is feature extraction, in this research we propose the combination of some feature extraction that is HOG, Gabor, LBP and use HSV color space. In next recognition stage some classifier are compared such as KNN, Random Forest, and Naïve Bayes. The propose method has been tasted on Indonesia local traffic sign. The results of the experimental work reveal that the approach of RGBN method showed precision and recall about 98,7% and 95,1% respectively in detecting traffic signs, and 100% for the precision and 86,7% for recall in recognizing process using K means Classifier.

Proposed System:



In this proposed method taking input from the video streaming.it can be defined as

VIDEO STREAMING:

Video streaming technology is one way to deliver video over the Internet. Using streaming technologies, the delivery of audio and video over the Internet can reach many millions of customer using their personal computers, PDAs, mobile smartphones or other streaming devices. The reasons for video streaming technology growth are:

- broadband networks are being deployed
- video and audio compression techniques are more efficient
- quality and variety of audio and video services over internet are increasing

There are two major ways for the transmission of video/audio information over the Internet:

Download mode. The content file is completely downloaded and then played. This mode requires long downloading time for the whole content file and requires hard disk space.

Streaming mode. The content file is not required to be downloaded completely and it is playing while parts of the content are being received and decoded.

By taking input from the video streaming given to pre-processing conversion. It converts RGB to GRAY scale image to Black and white image.

Pre-processing is a common name for operations with images at the lowest level of abstraction -- both input and output are intensity images. The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for

Blob Detection:

In computer vision, blob detection methods are aimed at detecting regions in a digital image that differ in properties, such as brightness or colour, compared to surrounding regions. Informally, a blob is a region of an image in which some properties are constant or approximately constant; all the points in a blob can be considered in some sense to be similar to each other. The most common method for blob detection is convolution.

CONCLUDING REMARKS

In this paper, we analyzed the GES automobile accident data from 1995 to 2000 and investigated the performance of neural network, decision tree, support vector machines and a hybrid decision tree – neural network based approaches to predicting drivers' injury severity in head-on front impact point collisions. The classification accuracy obtained in our experiments reveals that, for the non-incapacitating injury, the incapacitating injury, and the fatal injury classes, the hybrid approach performed better than neural network, decision trees and support vector machines.

REFERENCES

[1] Abdel-Aty, M., and Abdelwahab, H., Analysis and Prediction of Traffic Fatalities Resulting From Angle Collisions Including the Effect of Vehicles' Configuration and Compatibility. Accident Analysis and Prevention, 2003.

[2] Abdelwahab, H. T. and Abdel-Aty, M. A., Development of Artificial Neural Network Models

to Predict Driver Injury Severity in Traffic Accidents at Signalized Intersections. Transportation Research Record 1746, Paper No. 01-2234.

[3] Bedard, M., Guyatt, G. H., Stones, M. J., & Hireds, J. P., The Independent Contribution of Driver, Crash, and Vehicle Characteristics to Driver Fatalities. Accident analysis and Prevention, Vol. 34, pp. 717-727, 2002.

[4] Buzeman, D. G., Viano, D. C., & Lovsund, P., Car Occupant Safety in Frontal Crashes: A Parameter Study of Vehicle Mass, Impact Speed, and Inherent Vehicle Protection. Accident Analysis and Prevention, Vol. 30, No. 6, pp. 713-722, 1998.

[5] Dia, H., & Rose, G., Development and Evaluation of Neural Network Freeway Incident Detection Models Using Field Data. Transportation Research C, Vol. 5, No. 5, 1997, pp. 313-331.

[6] Evanco, W. M., The Potential Impact of Rural Mayday Systems on Vehicular Crash Fatalities. Accident Analysis and Prevention, Vol. 31, 1999, pp. 455-462.

[7] Hand, D., Mannila, H., & Smyth, P., Principles of Data Mining. The MIT Press, 2001.

[8] Kim, K., Nitz, L., Richardson, J., & Li, L., Personal and Behavioral Predictors of Automobile Crash and Injury Severity. Accident Analysis and Prevention, Vol. 27, No. 4, 1995, pp. 469-481.

[9] Kweon, Y. J., & Kockelman, D. M., Overall Injury Risk to Different Drivers: Combining Exposure, Frequency, and Severity Models. Accident Analysis and Prevention, Vol. 35, 2003, pp. 441-450.

[10] Martin, P. G., Crandall, J. R., & Pilkey, W. D., Injury Trends of Passenger Car Drivers In the USA. Accident Analysis and Prevention, Vol. 32, 2000, pp. 541-557.

[11] Mayhew, D. R., Ferguson, S. A., Desmond, K. J., & Simpson, G. M., Trends In Fatal Crashes Involving Female Drivers, 1975-1998. Accident Analysis and Prevention, Vol. 35, 2003, pp. 407-415.

[12] Mussone, L., Ferrari, A., & Oneta, M., An analysis of urban collisions using an artificial intelligence model. Accident Analysis and Prevention, Vol. 31, 1999, pp. 705-718.

[13] Ossiander, E. M., & Cummings, P., Freeway speed limits and Traffic Fatalities in Washington State. Accident Analysis and Prevention, Vol. 34, 2002, pp. 13-18.

[14] Shankar, V., Mannering, F., & Barfield, W., Statistical Analysis of Accident Severity on Rural Freeways. Accident Analysis and Prevention, Vol. 28, No. 3, 1996, pp.391-401.

[15] Sohn, S. Y., & Lee, S. H., Data Fusion, Ensemble and Clustering to Improve the Classification Accuracy for the Severity of Road Traffic Accidents in Korea. Safety Science, Vol. 4, issue1, February 2003, pp. 1-14.

[16] Tavris, D. R., Kuhn, E. M, & Layde, P. M., Age and Gender Patterns In Motor Vehicle Crash injuries: Improtance of Type of Crash and Occupant Role. Accident Analysis and Prevention, Vol. 33, 2001, pp. 167-172.

[17] Yang, W.T., Chen, H. C., & Brown, D. B., Detecting Safer Driving Patterns By A Neural Network Approach. ANNIE '99 for the Proceedings of Smart Engineering System Design Neural Network, Evolutionary Programming, Complex Systems and Data Mining, Vol. 9, pp 839-844, Nov. 1999.

[18] Zembowicz, R. and Zytkow, J. M., 1996. From Contingency Tables to Various Forms of Knowledge in Database. Advances in knowledge Discovery and Data Mining, editors, Fayyad, U. M., Piatetsky-Shapiro, G., Smyth, P., Uthurusamy, R. AAAI Press/The MIT Press, pp.329-349.

[19] Abraham, A., Meta-Learning Evolutionary Artificial Neural Networks, Neurocomputing Journal, Elsevier Science, Netherlands, Vol. 56c, pp. 1-38, 2004.

[20] Moller, A.F., A Scaled Conjugate Gradient Algorithm for Fast Supervised Learning, Neural Networks, Volume (6), pp. 525-533, 1993